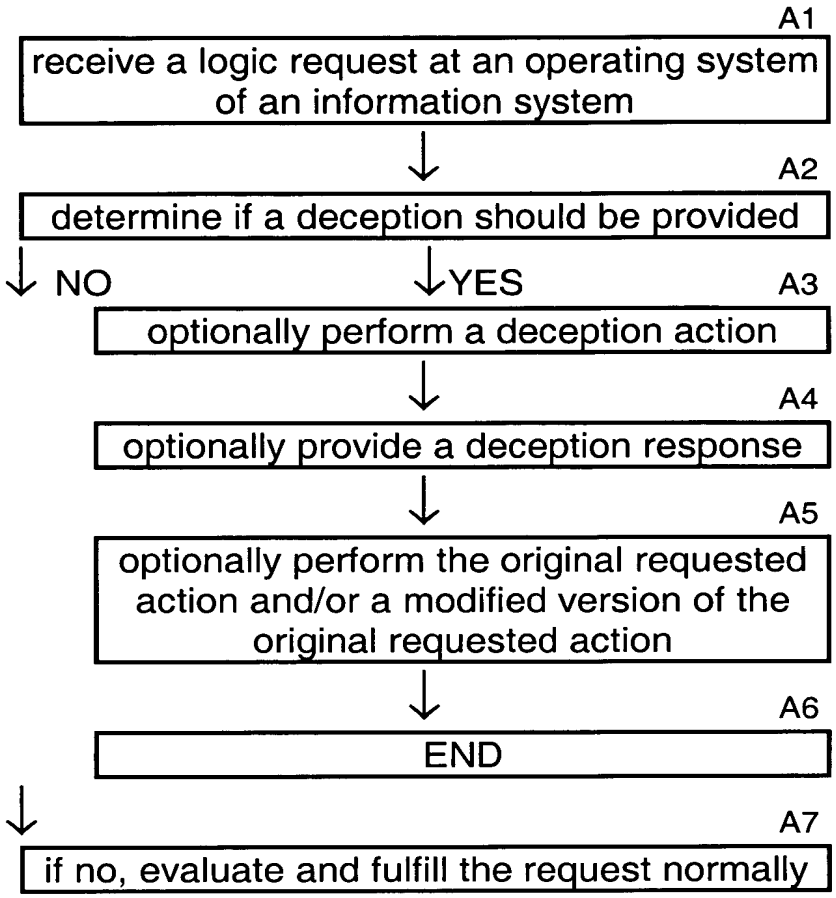
A1
receive a logic request at an operating system of an information system
A2
determine if a deception should be provided
NO
YES
A3
optionally perform a deception action
A4
optionally provide a deception response
A5
optionally perform the original requested action and/or a modified version of the original requested action
A6
END
A7
if no, evaluate and fulfill the request normally

FIG. 1

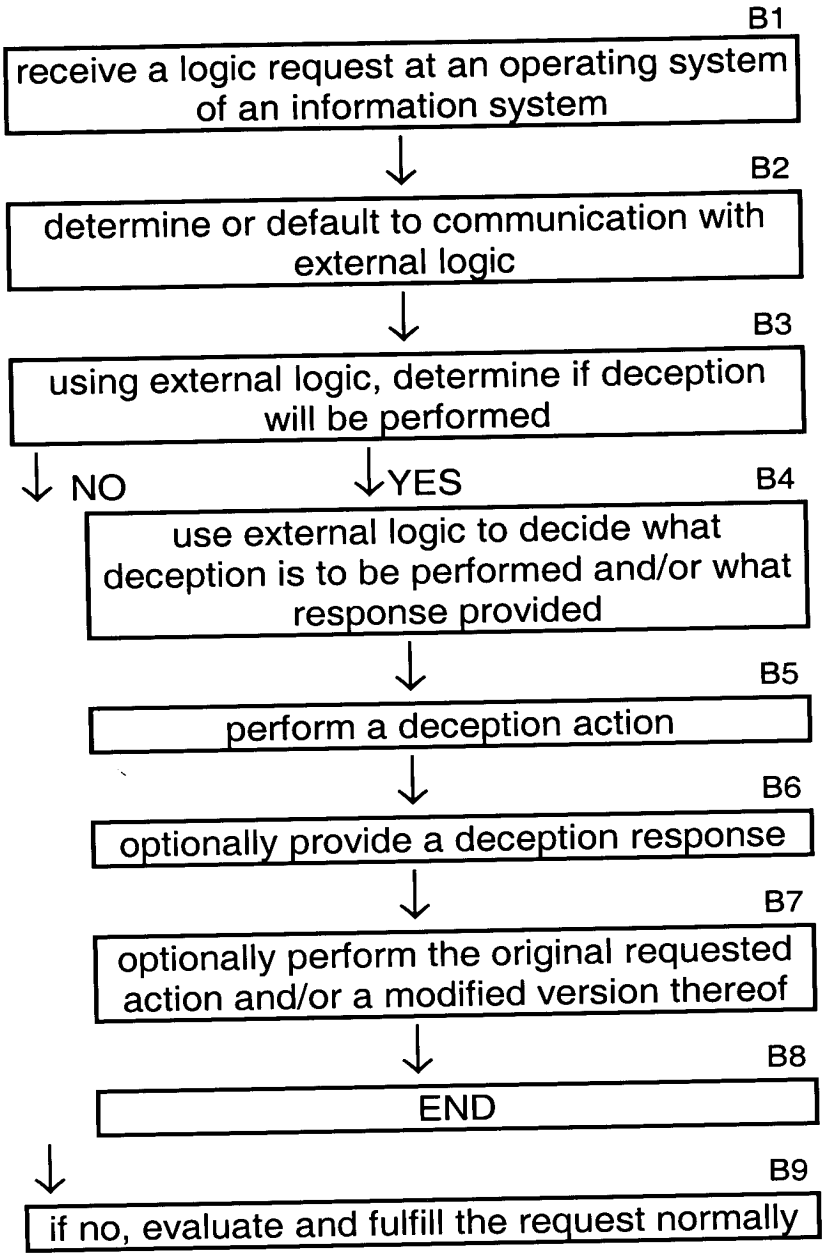
B1
receive a logic request at an operating system of an information system
B2
determine or default to communication with external logic
B3
using external logic, determine if deception will be performed
NO
YES
B4
use external logic to decide what deception is to be performed and/or what response provided
B5
perform a deception action
B6
optionally provide a deception response
B7
optionally perform the original requested action and/or a modified version thereof
B8
END
B9
if no, evaluate and fulfill the request normally

FIG. 2

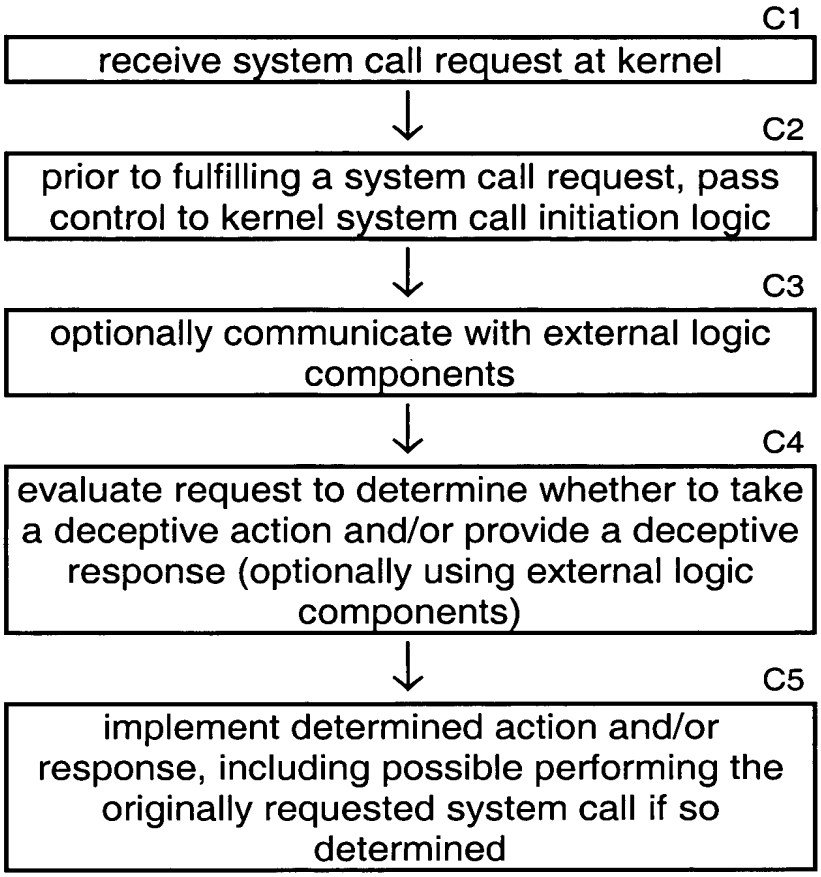
C1
receive system call request at kernel
C2
prior to fulfilling a system call request, pass control to kernel system call initiation logic
C3
optionally communicate with external logic components
C4
evaluate request to determine whether to take a deceptive action and/or provide a deceptive response (optionally using external logic components)
C5
implement determined action and/or response, including possible performing the originally requested system call if so determined

FIG. 3

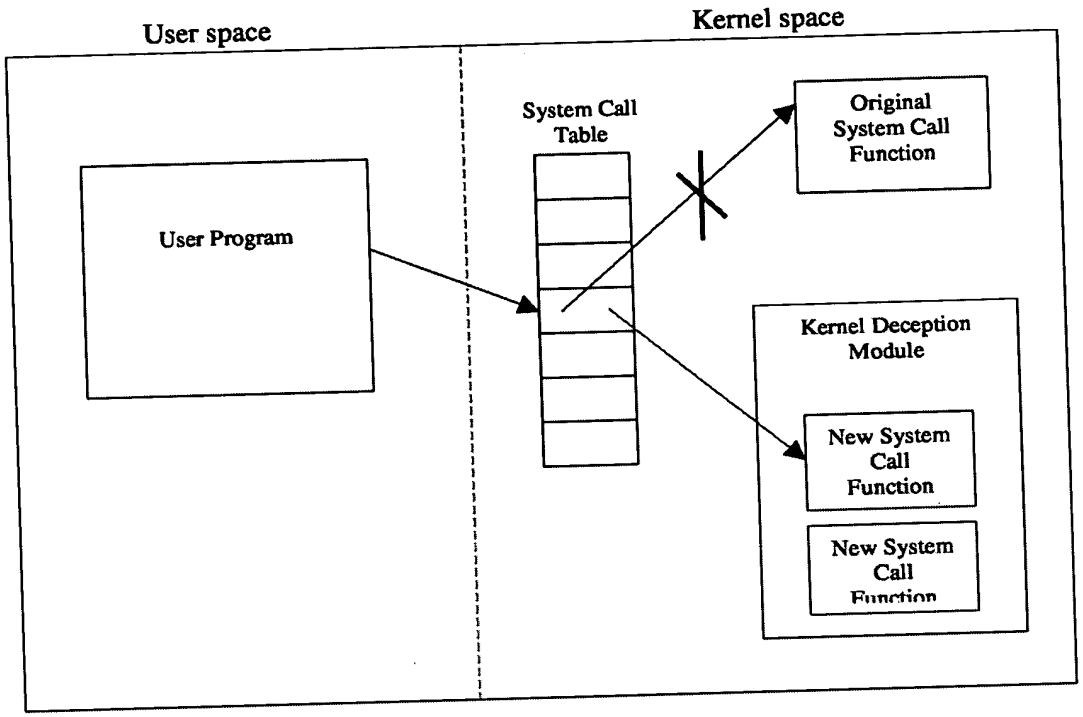
User space
Kernel space
System Call Table
Original System Call Function
User Program
Kernel Deception Module
New System Call Function
New System Call Function

FIG. 4

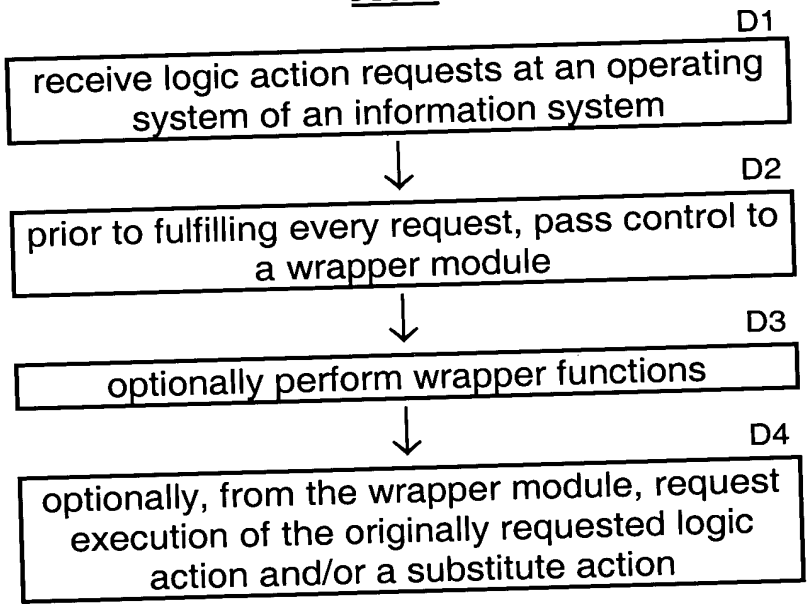
D1
receive logic action requests at an operating system of an information system
D2
prior to fulfilling every request, pass control to a wrapper module
D3
optionally perform wrapper functions
D4
optionally, from the wrapper module, request execution of the originally requested logic action and/or a substitute action

FIG. 5

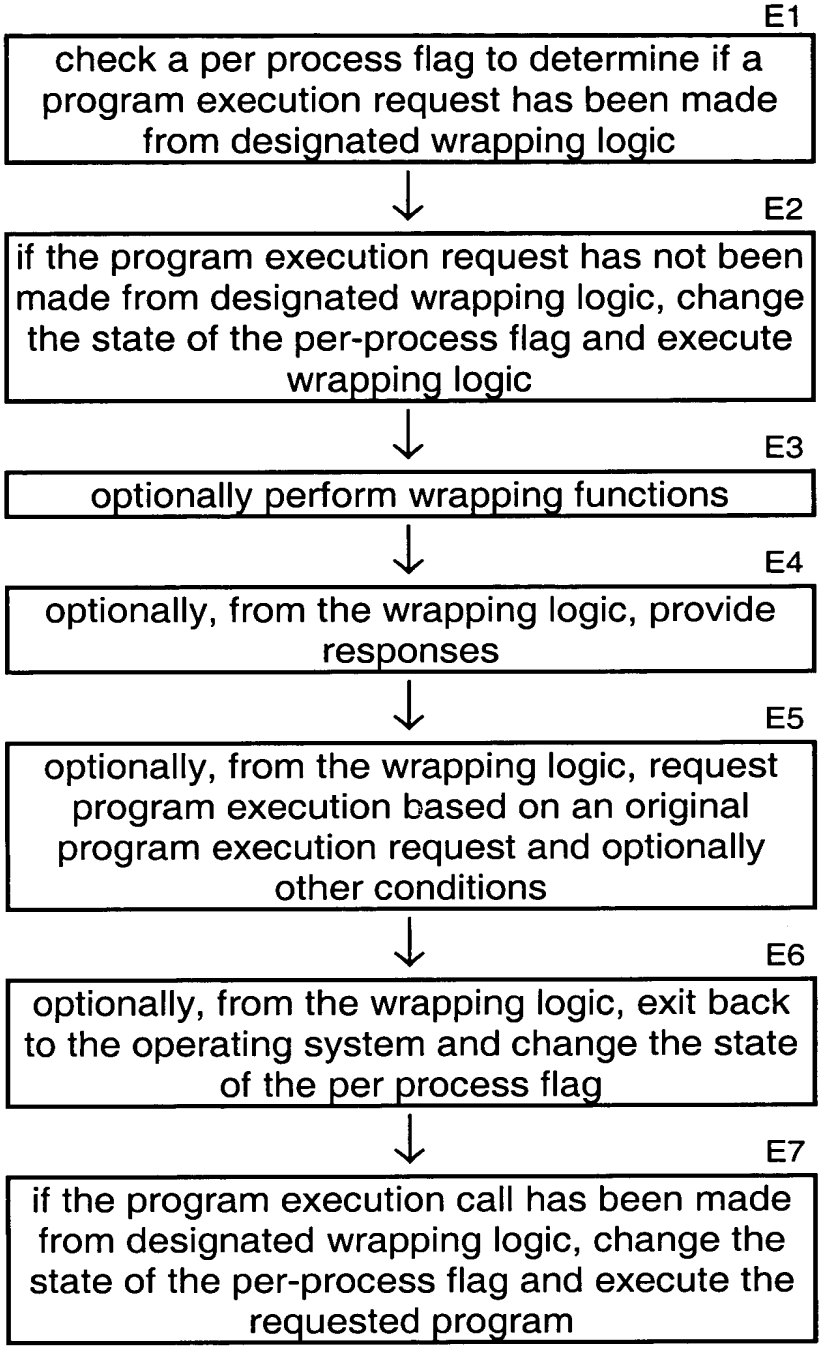
E1
check a per process flag to determine if a program execution request has been made from designated wrapping logic
E2
if the program execution request has not been made from designated wrapping logic, change the state of the per-process flag and execute wrapping logic
E3
optionally perform wrapping functions
E4
optionally, from the wrapping logic, provide responses
E5
optionally, from the wrapping logic, request program execution based on an original program execution request and optionally other conditions
E6
optionally, from the wrapping logic, exit back to the operating system and change the state of the per process flag
E7
if the program execution call has been made from designated wrapping logic, change the state of the per-process flag and execute the requested program

FIG. 6

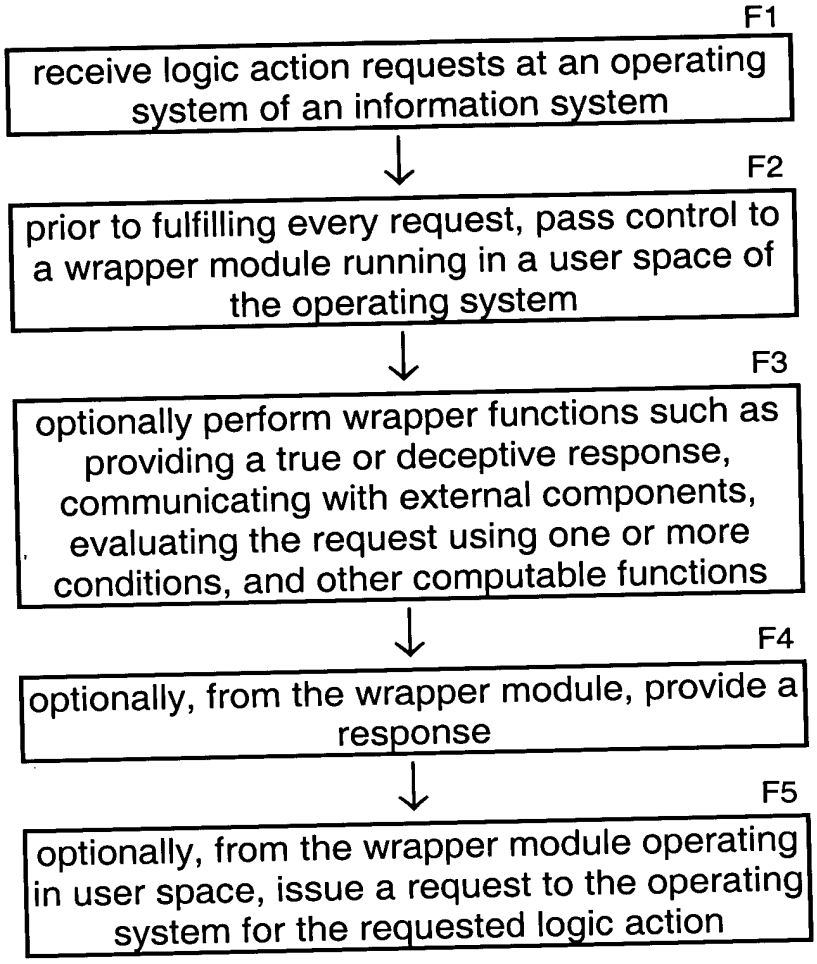
F1
receive logic action requests at an operating system of an information system
F2
prior to fulfilling every request, pass control to a wrapper module running in a user space of the operating system
F3
optionally perform wrapper functions such as providing a true or deceptive response, communicating with external components, evaluating the request using one or more conditions, and other computable functions
F4
optionally, from the wrapper module, provide a response
F5
optionally, from the wrapper module operating in user space, issue a request to the operating system for the requested logic action

FIG. 7

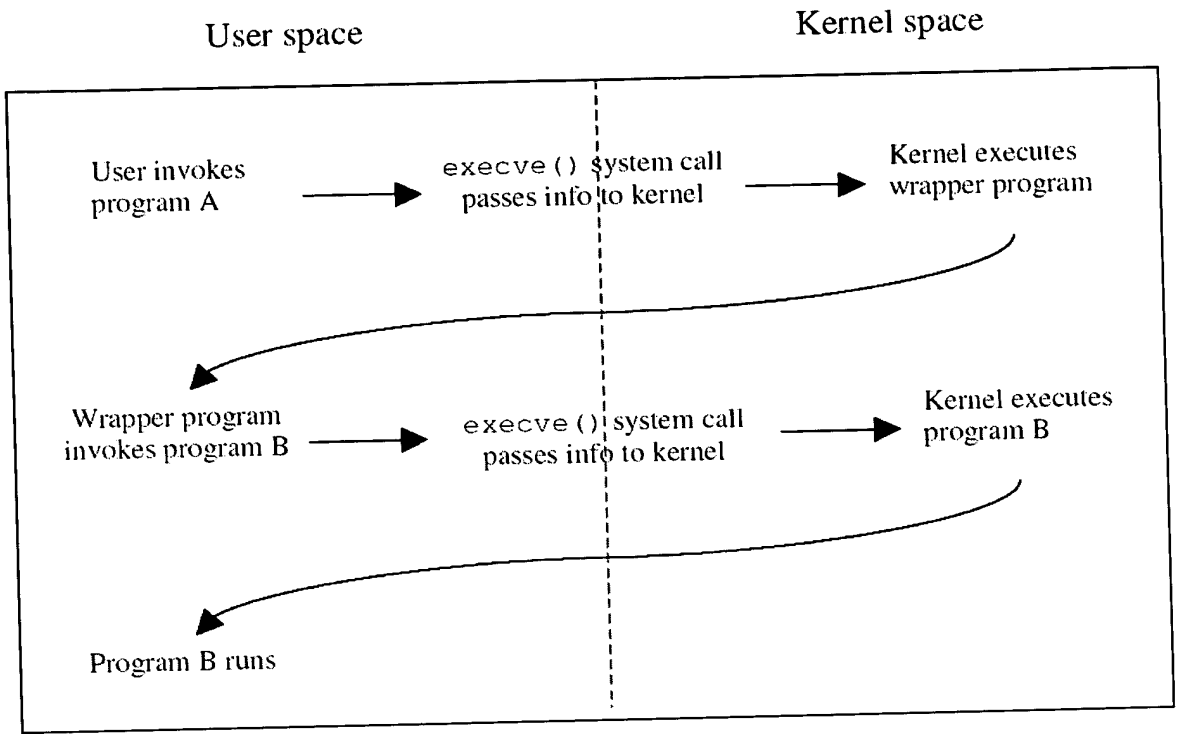
User space
Kernel space
User invokes program A
execve() system call passes info to kernel
Kernel executes wrapper program
Wrapper program invokes program B
execve() system call passes info to kernel
Kernel executes program B
Program B runs

FIG. 8

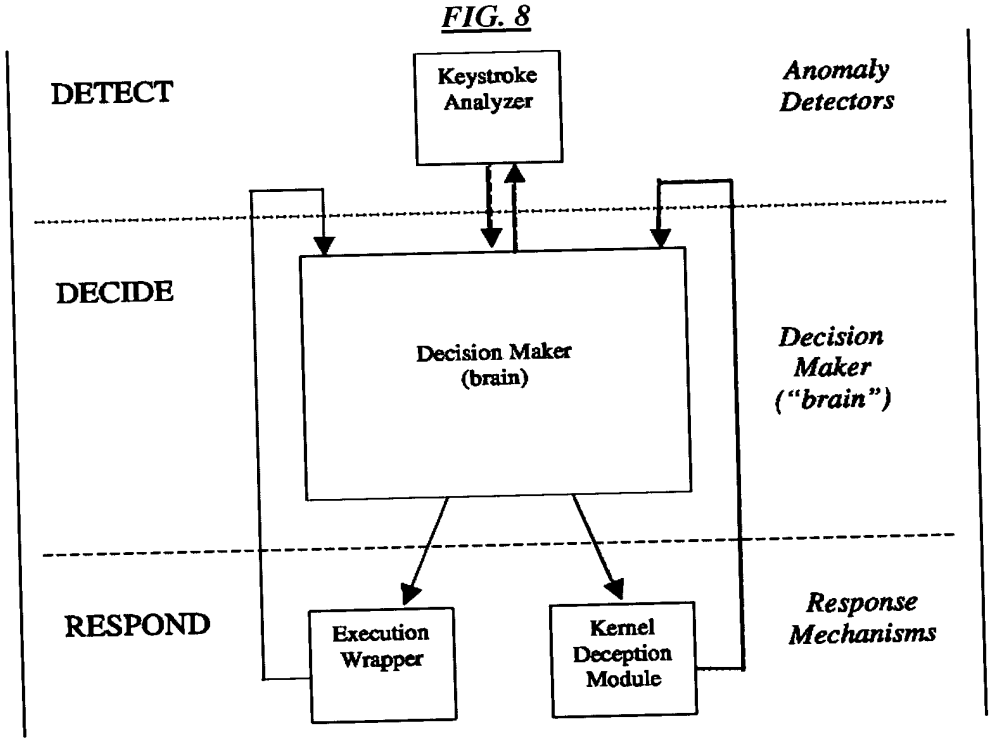
DETECT
Keystroke Analyzer
Anomaly Detectors
DECIDE
Decision Maker (brain)
Decision Maker ("brain")
RESPOND
Execution Wrapper
Kernel Deception Module
Response Mechanisms

FIG. 9

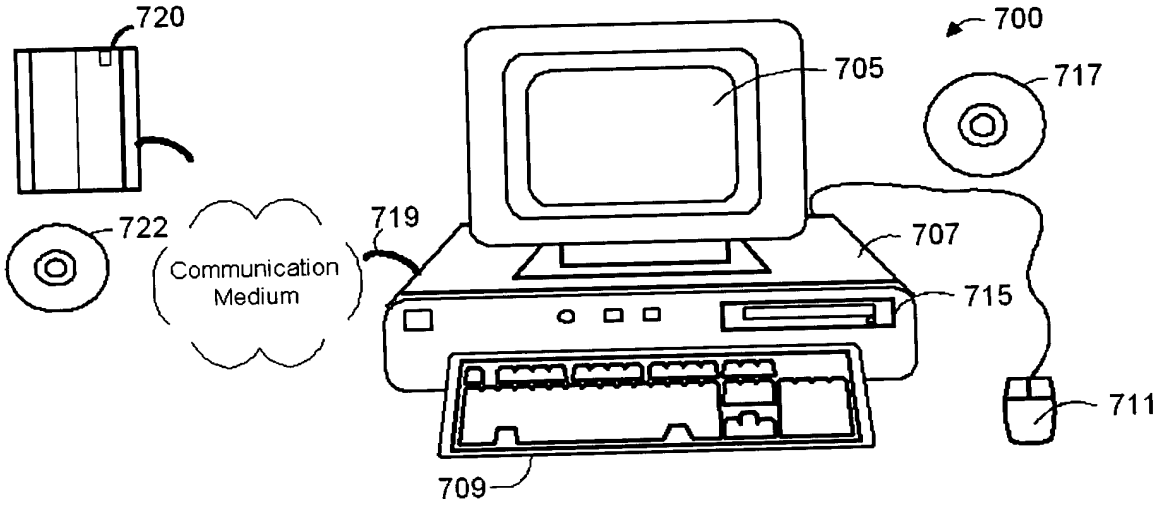
720
700
705
717
722
719
Communication Medium
707
715
711
709

FIG. 12

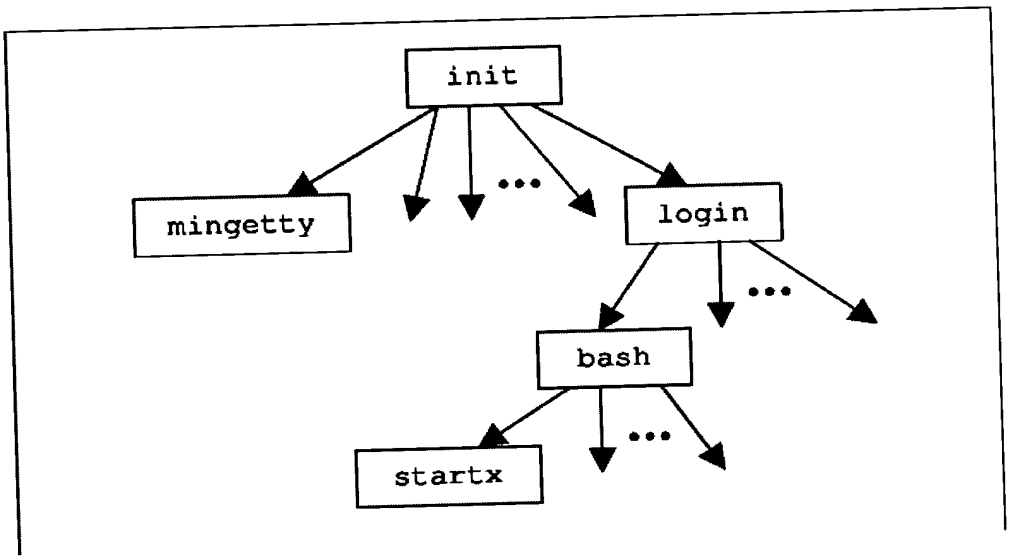
init
mingetty
login
bash
startx

FIG. 10

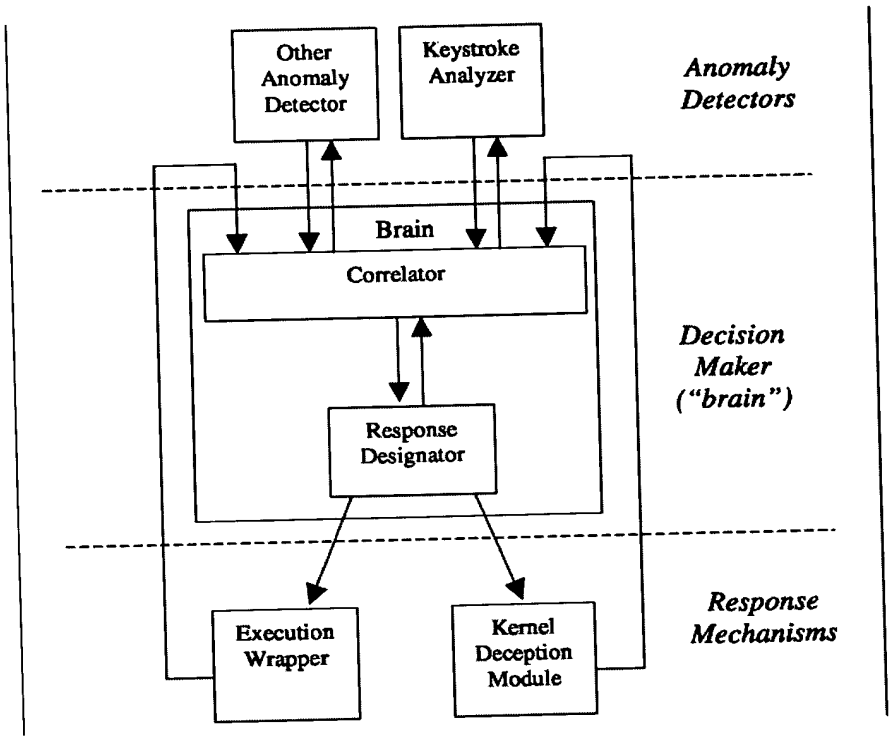
Other Anomaly Detector
Keystroke Analyzer
Anomaly Detectors
Brain
Correlator
Decision Maker ("brain")
Response Designator
Execution Wrapper
Kernel Deception Module
Response Mechanisms

FIG. 11